

Rec'd PCT/PTO 23 MAR 2005

PCT/JP03/12213 #2

25.09.03

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 4月 4日
Date of Application:

出願番号 特願2003-101085
Application Number:
[ST. 10/C]: [JP2003-101085]

REC'D 13 NOV 2003

WIPO

PCT

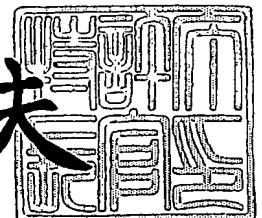
出願人 FDK株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年10月31日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 IP03527

【あて先】 特許庁長官 殿

【国際特許分類】 H03K 3/84

【発明者】

【住所又は居所】 東京都港区新橋5丁目36番11号 エフ・ディー・ケイ株式会社内

【氏名】 山本 博康

【発明者】

【住所又は居所】 東京都港区新橋5丁目36番11号 エフ・ディー・ケイ株式会社内

【氏名】 志賀 隆明

【発明者】

【住所又は居所】 東京都港区新橋5丁目36番11号 エフ・ディー・ケイ株式会社内

【氏名】 曾我 竜司

【発明者】

【住所又は居所】 東京都港区新橋5丁目36番11号 エフ・ディー・ケイ株式会社内

【氏名】 上遠野 昌良

【発明者】

【住所又は居所】 東京都港区新橋5丁目36番11号 エフ・ディー・ケイ株式会社内

【氏名】 渡邊 利幸

【特許出願人】

【識別番号】 000237721

【氏名又は名称】 エフ・ディー・ケイ株式会社

【代理人】

【識別番号】 100067046

【弁理士】

【氏名又は名称】 尾股 行雄

【電話番号】 03-3543-0036

【選任した代理人】

【識別番号】 100096862

【弁理士】

【氏名又は名称】 清水 千春

【電話番号】 03-3543-0036

【手数料の表示】

【予納台帳番号】 008800

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 物理乱数発生装置

【特許請求の範囲】

【請求項 1】 物理乱数発生器を有する物理乱数発生装置であって、
前記物理乱数発生器が、
基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を
備え、

シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、
パラレル乱数を保持しうる複数個のレジスターを備え、

前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レ
ジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記
レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了し
たレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新
する制御回路を備えたことを特徴とする物理乱数発生装置。

【請求項 2】 前記物理乱数発生器が、
複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き
込みアドレスを出力するアップ／ダウンカウンタを備え、

前記アップ／ダウンカウンタが出力した書き込みアドレスに基づき、パラレ
ル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備
え、

前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内
のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスター
へ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段
からパラレル乱数を読み出して出力するとともに、このレジスターより前段にあ
る各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたこと
を特徴とする請求項 1 に記載の物理乱数発生装置。

【請求項 3】 前記物理乱数発生器が、
前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総
数カウンタを備え、

前記総数カウンタがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えたことを特徴とする請求項 1 または請求項 2 に記載の物理乱数発生装置。

【請求項 4】 前記乱数検証回路の乱数検証方法として、
乱数値 “0” または “1” の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【請求項 5】 前記乱数検証回路の乱数検証方法として、
4 ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出された χ^2 乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【請求項 6】 前記乱数検証回路の乱数検証方法として、
連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【請求項 7】 前記乱数検証回路の乱数検証方法として、
所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【請求項 8】 チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファ機能をもつことを特徴とする請求項 1 から請求項 7 までのいずれかに記載の物理乱数発生装置。

【請求項 9】 前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにしたことを特徴とする請求項 1 から請求項 8 までのいずれかに記載の物理乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、各種の用途に用いるに好適な物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（例えば、CG、自動作曲）、制御、計測、FA、ロボット制御（人工知能）などが挙げられる。

【0002】

【従来の技術】

従来この種の物理乱数発生装置としては、半導体内で発生するノイズを用いたものが多く、パソコンに外部から接続して使用するよう構成される規模の大きなものや、ICチップ単体で乱数を発生させるものがあった。また、アミューズメント用には、時間的にランダムであると思わせる信号が発生した時に、備えられた高速カウンターの値を参照し、それを乱数として用いるものがあった。

【0003】

【発明が解決しようとする課題】

一般に物理乱数発生器は高速に乱数を発生することは難しく、時としてその乱数発生速度以上の大量の乱数が必要となる事が起こる。そのため、記憶媒体を設けて乱数を貯めておいたり、複数の物理乱数発生装置を用いで乱数の発生量を増やしたりすることが考えられるが、これを実現するためには複雑な回路を利用者側で組む必要が生じる。

【0004】

また、一般に物理乱数は使用環境によって乱数の質が変化する可能性があり、利用者がこれら物理乱数発生装置の発生した乱数が真正乱数として使用することができるか否かを確認することは有益なことである。しかしながら、乱数の検定を行うには専用の測定装置を構築しなければならず、一般の物理乱数発生装置利用者にとっては、このような余計なコストと手間がかかるような作業は受け入れ難い。また、乱数検定は大量のデータを扱うので、それを貯めておく記憶装置は

大容量のものが必要となるとともに、検定のための計算処理にも時間がかかる。

【0005】

本発明は、このような事情に鑑み、物理乱数発生装置単体での乱数利用効率が高く、かつ複数の物理乱数 IC を組み上げて乱数を高速に発生させることが容易であり、さらに、乱数の質を容易に確認して使用することが可能な物理乱数発生装置を提供することを目的とする。

【0006】

【課題を解決するための手段】

まず、本発明のうち請求項 1 に係る発明は、物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えて構成される。ここで、読出しクロックは基準クロックとは別に入力されるものである。

【0007】

また、本発明のうち請求項 2 に係る発明は、前記物理乱数発生器が、複数のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンタを備え、前記アップ／ダウンカウンタが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えて構成される。

【0008】

また、本発明のうち請求項3に係る発明は、前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えて構成される。

【0009】

また、本発明のうち請求項4に係る発明は、前記乱数検証回路の乱数検証方法として、乱数値“0”または“1”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【0010】

また、本発明のうち請求項5に係る発明は、前記乱数検証回路の乱数検証方法として、4ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出された χ 二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【0011】

また、本発明のうち請求項6に係る発明は、前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【0012】

また、本発明のうち請求項7に係る発明は、前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【0013】

また、本発明のうち請求項8に係る発明は、チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファ機能をも3ステートとして構成される。

【0014】

さらに、本発明のうち請求項 9 に係る発明は、前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにして構成される。

【0015】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図 1 は本発明に係る物理乱数発生装置の第 1 の実施形態を示す回路図、

図 2 は図 1 に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図、

図 3 は図 2 に示す物理乱数発生器の各部の出力波形を示す波形図、

図 4 は図 2 に示す物理乱数発生器の各部の出力波形を示す波形図、

図 5 は図 1 に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回路図、

図 6 は図 1 に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図、

図 7 は図 1 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図、

図 8 は図 1 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図、

図 9 は図 1 に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

【0016】

この物理乱数発生装置 91 は、図 1 に示すように、物理乱数発生器 1、乱数検証回路 21、制御回路 94、カウンタ 95、第 1 セレクター 96、第 2 セレクター 97 から構成されており、物理乱数発生器 1 は、図 2 に示すように、シリアル物理乱数発生器 2、カウンタ 3、シフトレジスタ 4、複数個（図 2 では m 個）のレジスタ 5、制御回路 6、アップ／ダウンカウンタ 7、セレクター 8、基準クロック側の 2 個の遅延回路 9 および読出しクロック側の 2 個の遅延回路 10 から構成されている。

【0017】

他方、乱数検証回路 21 は、図 5 から図 9 までに示すように、乱数検定規格 FIPS 140-2 に準拠した 4 種類の検定方法 (MonobitTest、PokerTest、RunsTest および LongRunsTest) に対応する部分から構成されている。すなわち、MonobitTest に関する部分は、図 5 に示すように、第 1 カウンター 23、第 2 カウンター 24、レジスター 25、制御回路 26 および比較器 27 から構成されており、PokerTest に関する部分は、図 6 に示すように、第 1 カウンター 33、シフトレジスター 34、デコーダー 35、複数個 (図 6 では 16 個) のカウンター 36、制御回路 37、セレクター 38、掛算器 39、加算器 40、レジスター 41 および比較器 42 から構成されている。また、RunsTest に関する部分はさらに乱数出力が “1” の場合と乱数出力が “0” の場合とに二分され、前者は、図 7 に示すように、第 1 カウンター 53、比較器 54、データ保持器 55、第 2 カウンター 56、制御回路 57、デコーダー 58、6 個のカウンター 59 および 6 個の比較器 60 から構成されており、後者は、図 8 に示すように、物理乱数発生器 1 のシリアル物理乱数発生器 2 からデコーダー 58 への出力線上にインバータが設けられて出力が反転する点を除き、前者と同じ構成を有している。さらに、LongRunsTest に関する部分は、図 9 に示すように、第 1 カウンター 73、比較器 74、データ保持器 75、制御回路 76、第 2 カウンター 77、第 1 比較器 78、レジスター 79 および第 2 比較器 80 から構成されている。

【0018】

物理乱数発生装置 91 は以上のような構成を有するので、この物理乱数発生装置 91 を作動させると、まず物理乱数発生器 1 で、シリアル乱数が出力されるとともに、パラレル乱数が保持されて必要に応じて出力できる状態となる。

【0019】

すなわち、基準クロック (CLK_0) でシリアル物理乱数発生器 2 より生成されたシリアル乱数 (SRND) をカウンター 3 のキャリーアウト (CO) に同期して、シフトレジスター 4 でシリアルからパラレルに変換した n ビットの乱数 (CRND) をセレクター 8 で選択されたレジスター 5 にロードしてパラレル乱数を保持する。

【0020】

このとき、セレクター 8 はアップ/ダウンカウンター 7 の出力の書込みアドレ

ス (ADDRESS) で指定されたレジスター 5 を選択し、カウンタ 3 のキャリーアウト (CO) に同期してパラレル乱数 (CRND) をレジスター 5 にロードし、ロードごとにアップ/ダウンカウンタ 7 をカウントアップし、アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) が m になった時点で、アップ/ダウンカウンタ 7 はカウントアップとパラレル乱数のロードを中止し、以降その状態を維持する。

【0021】

パラレル乱数の出力 (PRND) は最下位のレジスター 5 の出力とし、読み出し後に読出しクロック (CLK_R) を入力し、読出しクロックにてアップ/ダウンカウンタ 7 のカウントダウンとすべてのレジスター 5 内のデータを上位から下位へシフトし、パラレル乱数 (PRND) はその都度更新される。アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) がゼロになった時点で、アップ/ダウンカウンタ 7 はカウントダウンとデータシフトを中止し、以降その状態を維持する。

【0022】

アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) は外部に出力され、すべてのレジスター 5 に保持されているパラレル乱数の数を逐次モニター可能とする。

【0023】

遅延回路 9、10 は各クロックのエッジ (例えば、立上りエッジ) を取り出し、非常に短いパルス波形 (例えば、10 ns) を生成し、アップ/ダウンカウンタ 7 とすべてのレジスター 5 のクロック信号 (CLOCK)、アップ/ダウンカウンタ 7 の ENABLE 信号、すべてのレジスター 5 の SHIFT 信号と LOAD(0) ~ LOAD($m-1$) を生成する。これにより、基準クロック (CLK_0) と読出しクロック (CLK_R) が非同期または同期式で動作するときに、基準クロック (CLK_0) のエッジ (例えば、立上りエッジ) に対する読出しクロック (CLK_R) のエッジ (例えば、立上りエッジ) の禁止域 ($td_{Ra} + td_{0a} + 2 \times td_{mg}$) を非常に小さくして基準クロック (CLK_0) と読出しクロック (CLK_R) との干渉を最小限とすることができる。なお、CLK_0b と CLK_Rb がクロック信号 (CLOCK) を生成し、CLK_0a と CLK_Ra が ENABLE 信号、SHIFT 信号と LOAD(0) ~ LOAD($m-1$) を生成する。

【0024】

制御回路6はカウンタ3のキャリーアウト(CO)の同期信号(SYNC)、CLK_0a、CLK_Ra、アップ/ダウンカウンタ7のOVER信号とZERO信号より、アップ/ダウンカウンタ7のUP/DOWN信号とENABLE信号、すべてのレジスタ5のSHIFT信号とLOAD(0)～LOAD(m-1)用のLOAD信号を生成する。

【0025】

こうすることにより、基準クロックに同期してシリアル物理乱数発生器2で生成されたシリアル乱数よりn倍の周期で最大m個のnビットの平行乱数を保持することができる。それ以降のシリアル乱数は読み出し操作(CLK_Rの入力)をするまでは保持されない。こうして保持された最大m個の平行乱数は読出しクロックで必要なときに必要な量(最大m個)を短時間に集中して読み出すことができ、読み出された量の平行乱数は逐次補充される。基準クロック(CLK_0)のエッジに対する読出しクロックのエッジの禁止域が非常に狭く、非同期または同期式でタイミングよく、かつ効率的に読み出すことができる。書込みアドレスを読み出すことで、その時点で保持された平行乱数の量を確認することが可能となり、乱数を効率的に活用することができる。

【0026】

ところで、こうしてシリアル物理乱数発生器2で生成されたシリアル乱数は、乱数検定規格FIPS140-2に準拠した4種類の検定方法(MonobitTest、PokerTest、RunsTestおよびLongRunsTest)でその一様性が検証される。

【0027】

まず、MonobitTestによる検証が行われる。すなわち、図5に示すように、第1カウンタ23はスタート信号(START)と基準クロック(CLK_0)より制御回路26を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。第2カウンタ24は制御回路26の出力信号CLR_C2でスタート信号(START)が入った時点に初期化を行い、シリアル乱数(SRND)の“1”または“0”をカウントする。レジスタ25は制御回路26の出力信号LOAD_Rでスタート信号(START)が入った時点より20,000クロック時の第2カウンタ24のカウント値をロードして保持し、MonobitData(MOND)を出力する。比較器2

7はレジスタ25の出力MonobitData(MOND)と上限比較データ(例えば、10,275bit)および下限比較データ(例えば、9,725bit)とを比較し、MonobitJudge(MONJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にMonobitDataとMonobitJudgeを検証することができる。

【0028】

次に、PokerTestによる検証が行われる。すなわち、図6に示すように、第1カウンタ33はスタート信号(START)と基準クロック(CLK_0)より制御回路37を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。シフトレジスタ34はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次4ビットの平行乱数(PRND_4B)に変換する。デコーダ35は、スタート信号(START)と基準クロック(CLK_0)より制御回路37を介して生成されたENABLE信号がアクティブのとき(4クロックごとに1回)に平行乱数(PRND_4B)で指定された出力部(SE_0~SE_15)に出力される。カウンタ36は制御回路37の出力信号CLR_CRでスタート信号(START)が入った時点に初期化を行い、ENABLE信号がアクティブのとき(4クロックごとに1回)に平行乱数(PRND_4B)のデータにてデコーダ35で指定されたカウンタ36をカウントアップする。すべてのカウンタ36の総計は5,000カウントとなり、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にその間の4ビットごとの平行乱数(PRND_4B)のデータ(0~15)の度数分布データ(PokerData0~PokerData15)を取得する。レジスタ41は、制御回路37の出力信号CLR_CRでスタート信号(START)が入った時点に初期化(POKD=0)を行い、度数分布データ(PokerData0~PokerData15)を取得した後、セレクタ38、掛算器39、加算器40を介して度数分布データ(PokerData0~PokerData15)の16個の二乗和を求めることでPokerData(POKD)を取得する。比較器42はレジスタ41の出力PokerData(POKD)と上限比較データ(例えば、1,576,928)および下限比較データ(例えば、1,563,175)とを比較し、PokerJudge(POKJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000+16クロック後にPokerDataとPokerJudgeを検証

することができる。

【0029】

次いで、RunsTestによる検証が行われる。すなわち、図7および図8に示すように、第1カウンタ53はスタート信号(START)と基準クロック(CLK_0)より制御回路57を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器55はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次1ビット保持し、比較器54はシリアル乱数(SRND)とデータ保持器55で保持された乱数を比較し、1クロック前の乱数と今回の乱数が増加したときに信号CHANGEを出力する。第2カウンタ56は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号RUNS_Dを出力する。信号RUNS_Dと同一信号の長さ(L)の関係は $L = \text{RUNS_D} + 1$ となる。第2カウンタ56は、制御回路57の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化($\text{RUNS_D} = 0$)を行う。デコーダ58は、スタート信号(START)、基準クロック(CLK_0)、第1カウンタ53の出力(OUT_C)と比較器54の出力(CHANGE)より制御回路57を介して生成されたENABLE信号がアクティブ(CHANGEがアクティブ)のときで、図7ではシリアル乱数(SRND)が“1”のとき、図8ではシリアル乱数(SRND)が“0”のとき、第2カウンタ56の出力(RUNS_D)で選択された出力(SE_1～SE_6+)をアクティブにする。なお、 $L=1 \rightarrow \text{SE}_1$ 、 $L=2 \rightarrow \text{SE}_2$ 、…、 $L=6+ \rightarrow \text{SE}_{6+}$ となる。すべてのカウンタ59は、制御回路57の出力信号CLR_Cでスタート信号(START)が入った時点に初期化を行い、デコーダ58の出力(SE_1～SE_6+)で指定されたカウンタ59をカウントアップし、1～6+の同一信号の長さ(L)の出現回数(図7ではRunsData1H～RunsData6+H、図8ではRunsData1L～RunsData6+L)を取得する。各比較器60は各カウンタ59の出力(図7ではRunsData1H～RunsData6+H、図8ではRunsData1L～RunsData6+L)とそれぞれの上限比較データ(例えば、2,685、1,386、723、384、209、209)および下限比較データ(例えば、2,315、1,114、527、240、103、103)とを比較し、判定信号(図7ではRunsJudge1H～RunsJudge6+H、図8ではRunsJudge1L～RunsJudge6+L)を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後に

RunsTestのデータと判定を検証することができる。

【0030】

最後に、LongRunsTestによる検証が行われる。すなわち、図9に示すように、第1カウンタ73はスタート信号(START)と基準クロック(CLK_0)より制御回路57を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器75はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次1ビット保持し、比較器74はシリアル乱数(SRND)とデータ保持器75で保持された乱数を比較し、1クロック前の乱数と今回の乱数が増減したときに信号CHANGEを出力する。第2カウンタ77は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号LRUNS_Dを出力する。第2カウンタ77は、制御回路76の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(LRUNS_D=0)を行う。レジスタ79は、制御回路76の出力信号CLR_Rでスタート信号(START)が入ったときに初期化(LRUNS_D=0)を行う。レジスタ79の出力信号LongRunsData(LRND)と第2カウンタ77の出力信号(LRUNS_D)を第1比較器78で比較し、 $LRND < LRUNS_D$ のときに第1比較器78は出力信号COMP_Uを出力し、制御回路76を介してレジスタ79にLOAD_R信号を出力して、レジスタ79に逐次LRUNS_Dの最大値を保持する。第2比較器80は上限比較データ(例えば、26)と比較し、判定信号LongRunsJudge(LRNJ)を出力する。信号LRUNS_D、LRNDと同一信号の長さ(L)の関係は $L = LRUNS_D + 1$ 、 $L(max) = LRND + 1 = LRUNS_D(max) + 1$ となる。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にLongRunsTestのデータと判定を検証することができる。

【0031】

そして、こうして4種類の検定方法で検証された一様性乱数の検証データは、図1に示すように、第2セレクタ97に保持され、使用者の要望に応じて出力される。選択信号(A0、A1)と動作テーブルを表1に示す。

【表 1】

ADDRE_S	A1	A0	読出しクロック (CLK_R) の働き	出力 (DATA BUS)
0	0	0	パラレル物理乱数の更新	パラレル物理乱数
1	0	1	パラレル物理乱数の更新	パラレル物理乱数の生成状態
2	1	0	乱数検証のスタート/カウンターの初期化	乱数検証状態/モニターアドレス
3	1	1	乱数検証のモニターアドレス更新	乱数検証結果/検証データ

【0032】

すなわち、物理乱数発生器 1 は、選択信号 (A1) の状態 (“0” または “1”) により、読出しクロック (CLK_R) でのパラレル乱数の更新 (アップ/ダウンカウンタ 7 のカウントダウン) または非更新とする。出力のパラレル乱数 (PRND) は第 2 セレクター 97 の DATA_0 に接続される。出力 (COND_R) には書込みアドレス (ADDRESS) などの物理乱数生成時およびパラレル乱数変換時に生成される各種データやフラグを出力し、第 2 セレクター 97 の DATA_1 に接続される。

【0033】

乱数検証回路 21 は、選択信号 (A0、A1) が 2 (ADDRE_S) のときに制御回路 94 を介して読出しクロック (CLK_R) 信号で検証を開始し、MonobitTest、PokerTest、RunsTest および LongRunsTest を基準クロック (CLK_0) で 20,000+16 サイクルで完了し、判定結果、判定データ、PokerTest の生データを出力して第 1 セレクター 96 に接続される。その詳細を表 2 に示す。

【表 2】

モニターアドレス (SEL_ADD)	出力 (DATA BUS)
0	0 ; Monobit Judge (MONJ) 1 ; Poker Judge (POKJ) 2 ; Runs Judge 1H (RUNJ1H) 3 ; Runs Judge 1L (RUNJ1L) 4 ; Runs Judge 2H (RUNJ2H) 5 ; Runs Judge 2L (RUNJ2L) 6 ; Runs Judge 3H (RUNJ3H) 7 ; Runs Judge 3L (RUNJ3L) 8 ; Runs Judge 4H (RUNJ4H) 9 ; Runs Judge 4L (RUNJ4L) 10 ; Runs Judge 5H (RUNJ5H) 11 ; Runs Judge 5L (RUNJ5L) 12 ; Runs Judge 6+H (RUNJ6+H) 13 ; Runs Judge 6+L (RUNJ6+L) 14 ; Long Run Judge (LRNJ) 15 ; 総合判定
1	Monobit Data (MOND)
2	Poker Data (POKD)
3	Runs Data 1H (RUND1H)
4	Runs Data 1L (RUND1L)
5	Runs Data 2H (RUND2H)
6	Runs Data 2L (RUND2L)
7	Runs Data 3H (RUND3H)
8	Runs Data 3L (RUND3L)
9	Runs Data 4H (RUND4H)
10	Runs Data 4L (RUND4L)
11	Runs Data 5H (RUND5H)
12	Runs Data 5L (RUND5L)
13	Runs Data 6+H (RUND6+H)
14	Runs Data 6+L (RUND6+L)
15	Long Run Data (LRND)
16	Poker Data 0 (POK_0)
17	Poker Data 1 (POK_1)
18	Poker Data 2 (POK_2)
19	Poker Data 3 (POK_3)
20	Poker Data 4 (POK_4)
21	Poker Data 5 (POK_5)
22	Poker Data 6 (POK_6)
23	Poker Data 7 (POK_7)
24	Poker Data 8 (POK_8)
25	Poker Data 9 (POK_9)
26	Poker Data 10 (POK_10)
27	Poker Data 11 (POK_11)
28	Poker Data 12 (POK_12)
29	Poker Data 13 (POK_13)
30	Poker Data 14 (POK_14)
31	Poker Data 15 (POK_15)

【0034】

なお、総合判定はすべての判定結果が合格のときに出力される。出力 (COND_T)

には、乱数検証時に生成される各種データやフラグを出力し、第2セレクター97のDATA_2にカウンター出力のモニターアドレス(SEL_ADD)とともに接続される。また、検証のスタート信号にてパラレル乱数生成用のカウンター3、シフトレジスター4、アップ/ダウンカウンター7とすべてのレジスター5は初期化され、検証された物理乱数を保持して検証後の物理乱数を使用することができる。

【0035】

カウンター95は第1セレクター96のモニターアドレス(SEL_ADD)を生成する。カウンター95は、制御回路94の出力信号(CLR_C)で選択信号(A0、A1)が2(ADDRE_S)のときに読出しクロック(CLK_R)信号で検証を開始し、この開始時に初期化を行い、制御回路94の出力信号(CLK_C)で選択信号(A0、A1)が3(ADDRE_S)のときに読出しクロック(CLK_R)信号でカウンター95のカウントアップ(更新)を行う。

【0036】

これにより、基準クロックに同期して生成されたシリアル乱数(SRND)と逐次補充されるパラレル乱数(PRND)の生成および一様性の検証を逐次行うことができる。

【0037】

こうすることにより、物理乱数発生器1の検証およびデータの確認が容易となり、検証後の乱数を活用することができる。選択信号(A0、A1)と第2セレクター97を用いることで入出力端子を大幅に減らすことができる。選択信号(A0、A1)、読出しクロック(CLK_R)、カウンター95と第2セレクター97で、参照できる有効な検証データを拡大することができる。

【0038】

なお、図10に示すように、物理乱数発生器1にチップセレクト(CS)と出力イネーブル(OE)の入力を付加し、パラレル乱数[PRND(0)~PRND(n-1)]の出力形態を3ステート(“0”、“1”、off)にすることもできる。

【0039】

また、図11および図12に示すように、複数個(図11ではp個)の物理乱数発生器1とセレクター12とで高速(図11ではp倍)の乱数生成スピードを

獲得することも可能である。ここで、基準クロック (CLK_0) のエッジ (例えば、立上りエッジ) に対する読出しクロック (CLK_R) のエッジ (例えば、立上りエッジ) の禁止域 ($td_Ra + td_0a + 2 \times td_mg$) を非常に狭く考慮することのみで非同期または同期式の高速乱数発生を容易に実現することができる。

【0040】

このように、チップセレクト (CS) と出力イネーブル (OE) を有することで、物理乱数発生器 1 を複数個接続することが容易となり、乱数生成の高速化が可能となる。また、チップセレクト (CS) と出力イネーブル (OE) を有することで、CPU を使用したシステムに物理乱数発生器 1 を容易に接続することができる。

【0041】

なお、上述の実施形態では、基準クロック (CLK_0) のエッジに対する読出しクロック (CLK_R) のエッジの禁止域 ($td_Ra + td_0a + 2 \times td_mg$) を非常に小さくして基準クロック (CLK_0) と読出しクロック (CLK_R) との干渉を最小限とするため、基準クロック側および読出しクロック側にそれぞれ 2 個の遅延回路 9、10 を設けた場合について説明したが、基準クロック側と読出しクロック側のいずれか一方にだけ遅延回路 9、10 を設けてもよく、遅延回路 9、10 の個数も 1 個以上であれば何個でも構わない。或いはまた、遅延回路 9、10 に代えて波形成形回路 (例えば、単安定マルチバイブレータ) を付加しても、同じ効果を得ることができる。

【0042】

(付記 1) 物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えたことを特徴とする物理乱数発生装置。

【0043】

(付記2) 前記物理乱数発生器が、複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ/ダウンカウンタを備え、前記アップ/ダウンカウンタが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード信号に基づいて前記シリアル/パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたことを特徴とする請求項1に記載の物理乱数発生装置。

【0044】

(付記3) 前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンタを備え、前記総数カウンタがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えたことを特徴とする請求項1または請求項2に記載の物理乱数発生装置。

【0045】

(付記4) 付記1～3に記載の物理乱数発生装置において、乱数生成用の基準クロックと読出しクロックのいずれか一方または双方に遅延回路または波形成形回路を付加してクロックのエッジを抽出して基準クロックのエッジに対する読出しクロックのエッジの禁止域を最小にするようにしたことを特徴とする物理乱数発生装置。

【0046】

(付記5) 前記乱数検証回路の乱数検証方法として、乱数値“0”または“1”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項3に記載の物理乱数発生装置。

【0047】

(付記 6) 前記乱数検証回路の乱数検証方法として、4 ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出された χ 二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【0048】

(付記 7) 前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【0049】

(付記 8) 前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 3 に記載の物理乱数発生装置。

【0050】

(付記 9) チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファ機能を 3 ステートとしたことを特徴とする請求項 1 から請求項 7 までのいずれかに記載の物理乱数発生装置。

【0051】

(付記 10) 付記 9 に記載の物理乱数発生装置において、第 1 セレクター、カウンタを有して選択信号 (A0 = “0”、A1 = “1”) の時には乱数検証状態とモニターアドレスを出力し、選択信号 (A0 = “1”、A1 = “1”) の時には乱数の判定結果と検証データを出力し、読出しクロックでモニターアドレスの更新を行なうようにしたことを特徴とする物理乱数発生装置。

【0052】

(付記 11) 付記 10 に記載の物理乱数発生装置において、一様性乱数の Poker Test の度数分布データを出力するようにしたことを特徴とする物理乱数発生装置。

【0053】

(付記 12) 付記 9 ～ 11 に記載の物理乱数発生装置において、読出しクロックにて一様性乱数検証のスタート時に平行乱数の保持に関連した回路 (カウン

ター、シフトレジスター、アップ／ダウンカウンタ、レジスター)の初期化を行い、すべての保持されたパラレル乱数が一様性乱数の検証済みの乱数を出力するようにしたことを特徴とする物理乱数発生装置。

【0054】

(付記13)前記物理乱数発生器を複数個用意し、セレクトのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力することを特徴とする請求項1から請求項8までのいずれかに記載の物理乱数発生装置。

【0055】

【発明の効果】

以上説明したように、本発明のうち請求項1～7に係る発明によれば、生成された物理乱数を効率よく利用することができるとともに、その乱数の一様性を容易に検定して使用することができ、かつ、簡単な回路構成によりこれらを実現することが可能となる。

【0056】

また、本発明のうち請求項8、9に係る発明によれば、複数個の物理乱数発生ICを用いて高速に乱数を発生させることが容易となり、かつ、Data Busに直接接続できるようになるため、物理乱数発生装置の使いやすさが格段に向上する。

【図面の簡単な説明】

【図1】

本発明に係る物理乱数発生装置の第1の実施形態を示す回路図である。

【図2】

図1に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図である。

【図3】

図2に示す物理乱数発生器の各部の出力波形を示す波形図である。

【図4】

図2に示す物理乱数発生器の各部の出力波形を示す波形図である。

【図5】

図1に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回

路図である。

【図 6】

図 1 に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図である。

【図 7】

図 1 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図である。

【図 8】

図 1 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図である。

【図 9】

図 1 に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

【図 10】

本発明に係る物理乱数発生装置の第 2 の実施形態を示す回路図である。

【図 11】

本発明に係る物理乱数発生装置の第 3 の実施形態を示す回路図である。

【図 12】

図 11 に示す物理乱数発生装置の各部の出力波形を示す波形図である。

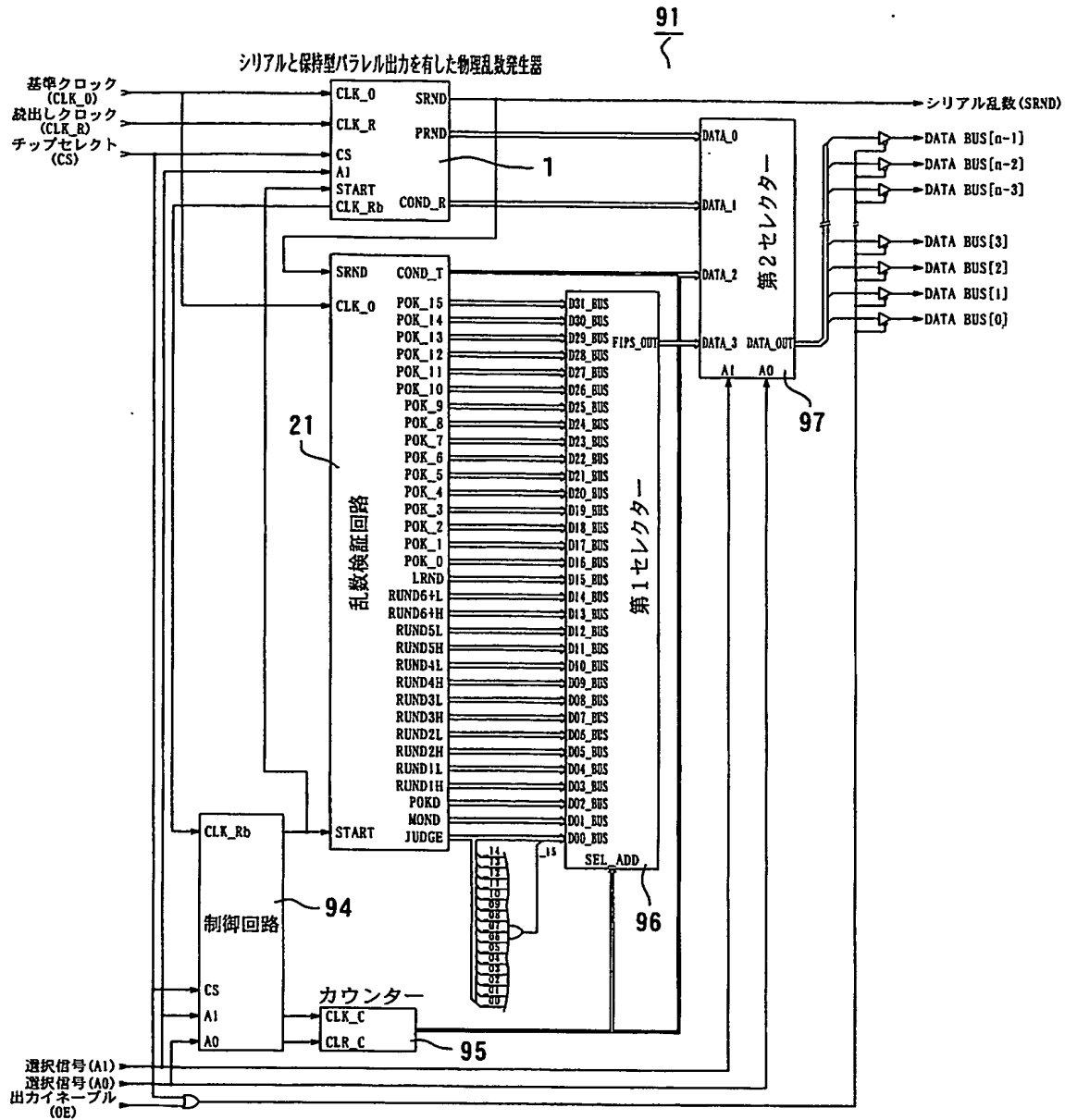
【符号の説明】

- 1 ……物理乱数発生器
- 2 ……シリアル物理乱数発生器
- 4 ……シリアル／パラレル変換部（シフトレジスター）
- 5 ……レジスター
- 6 ……制御回路
- 7 ……アップ／ダウンカウンタ
- 8、12 ……セレクター
- 23、33、53、73 ……総数カウンタ（第 1 カウンタ）
- 26、37、57、76 ……乱数検証回路（制御回路）

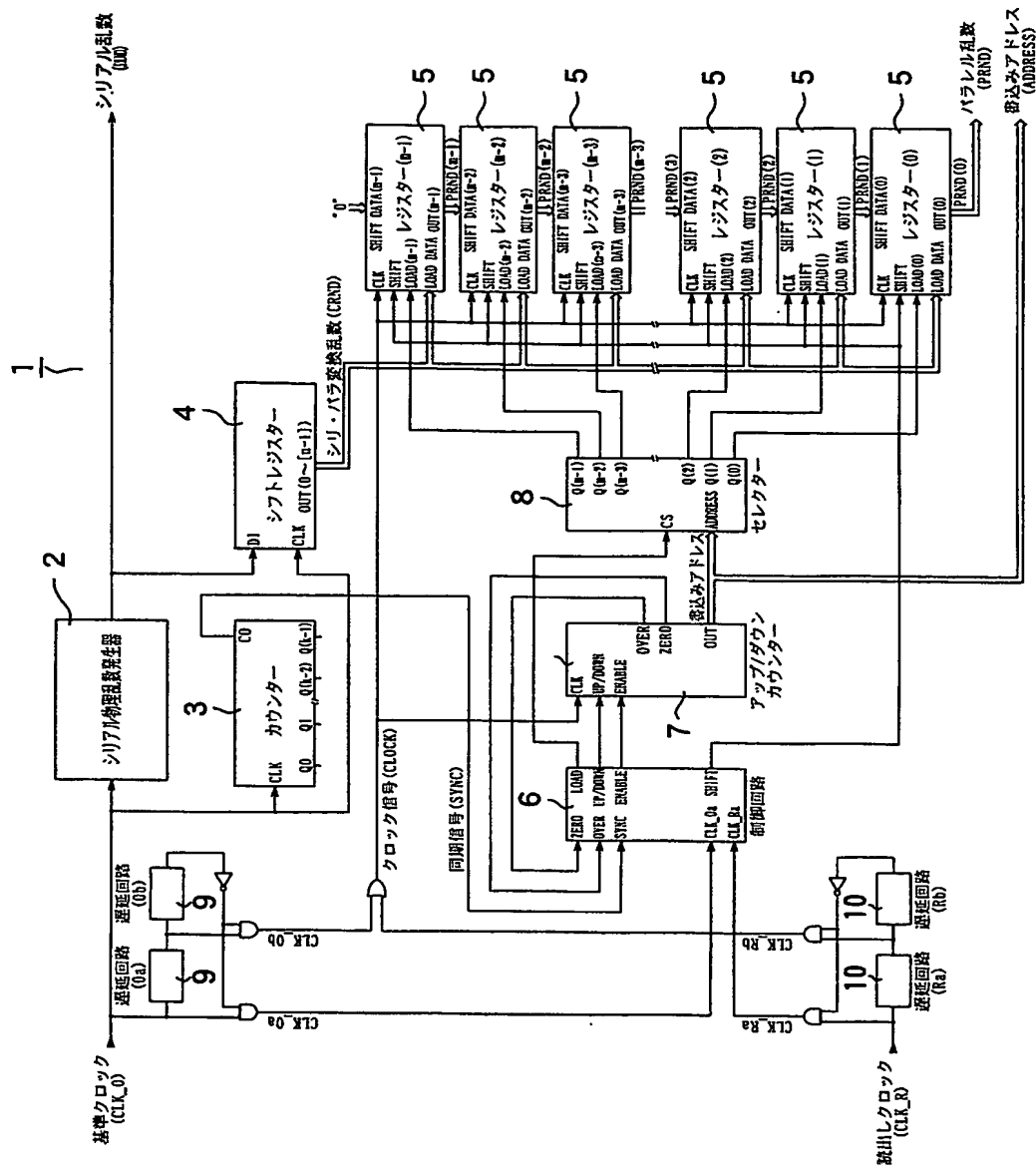
9 1物理乱数発生装置

【書類名】 図面

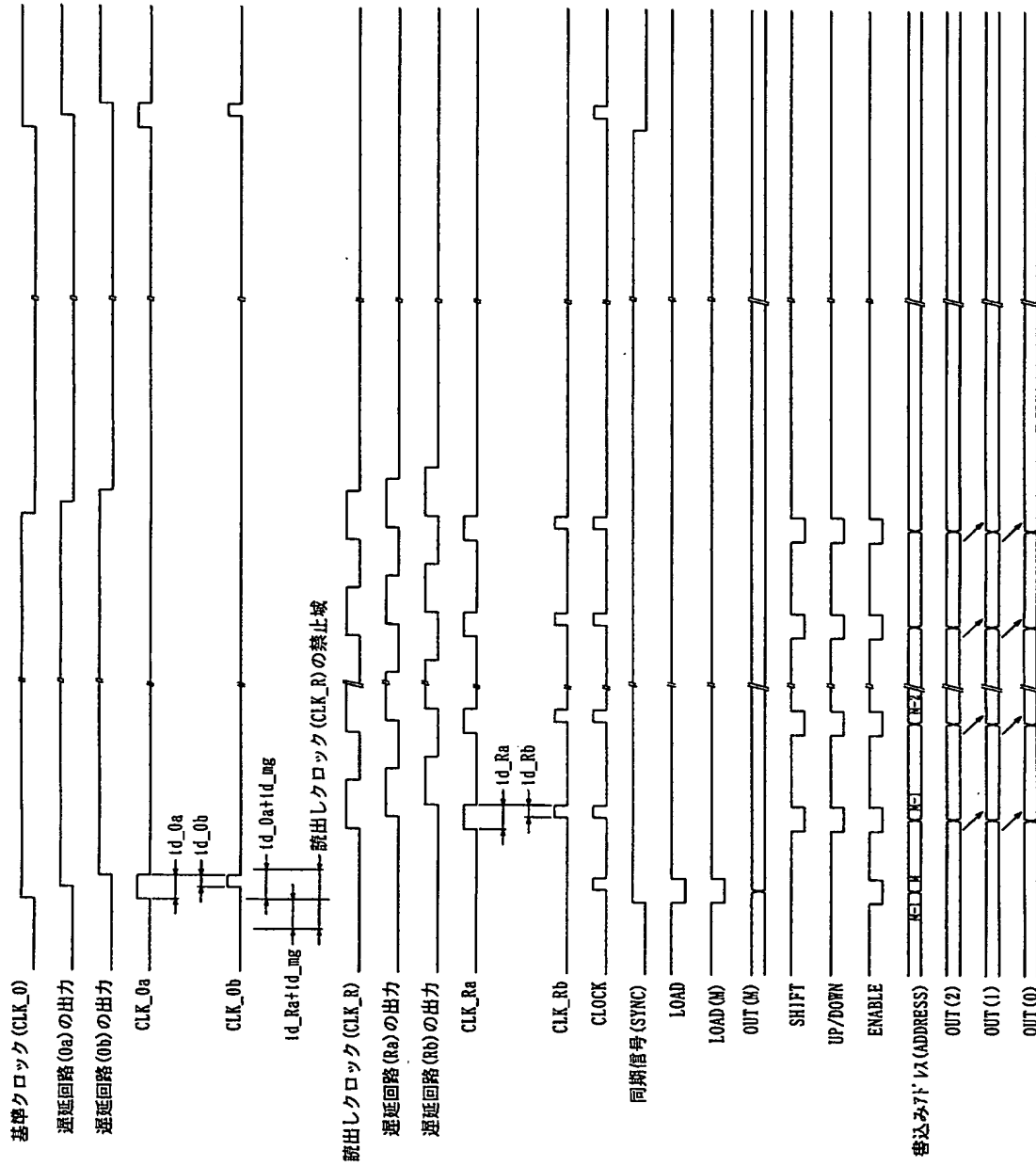
【図 1】



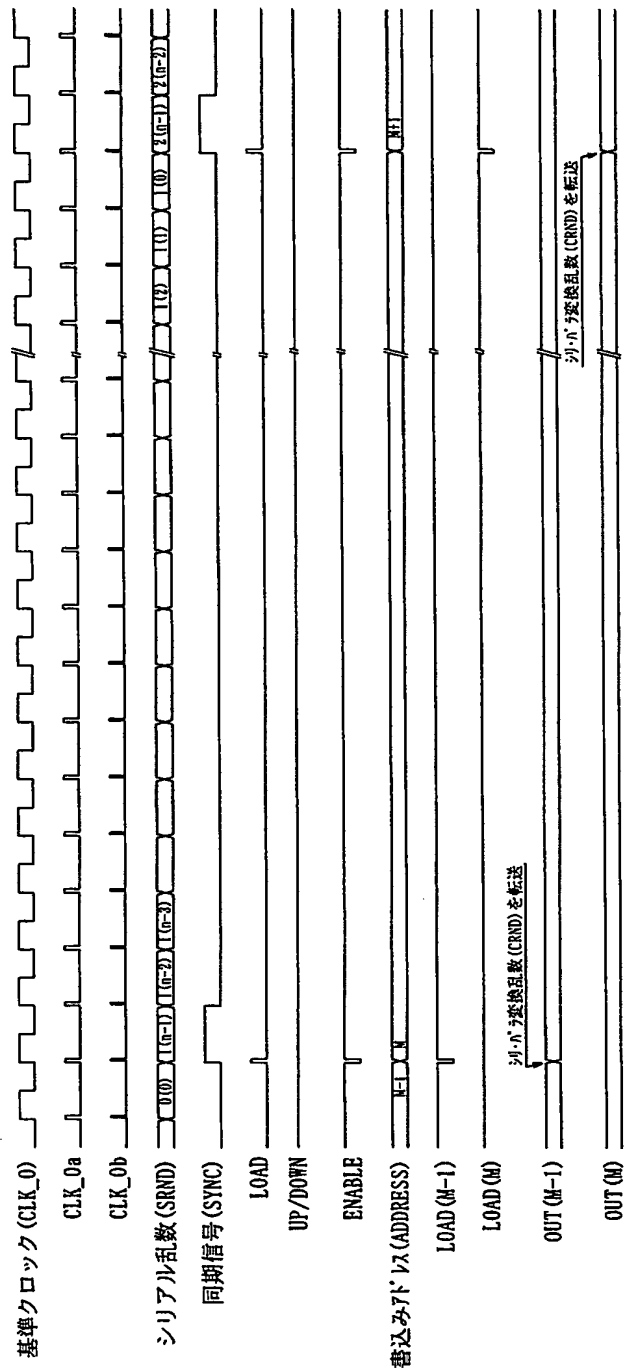
【図2】



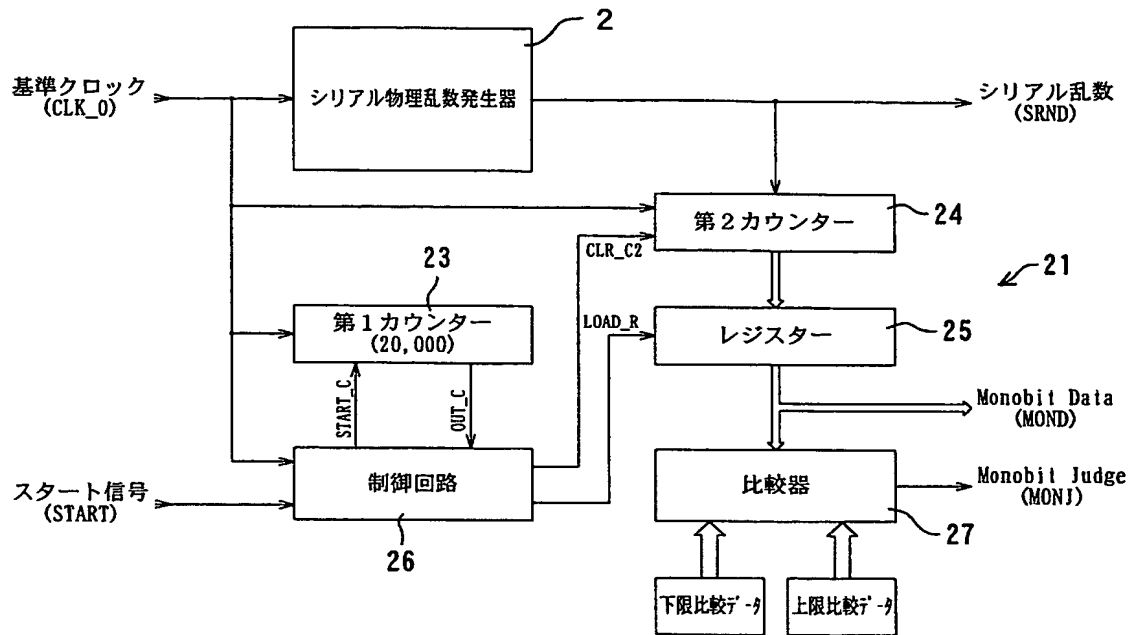
【図 3】



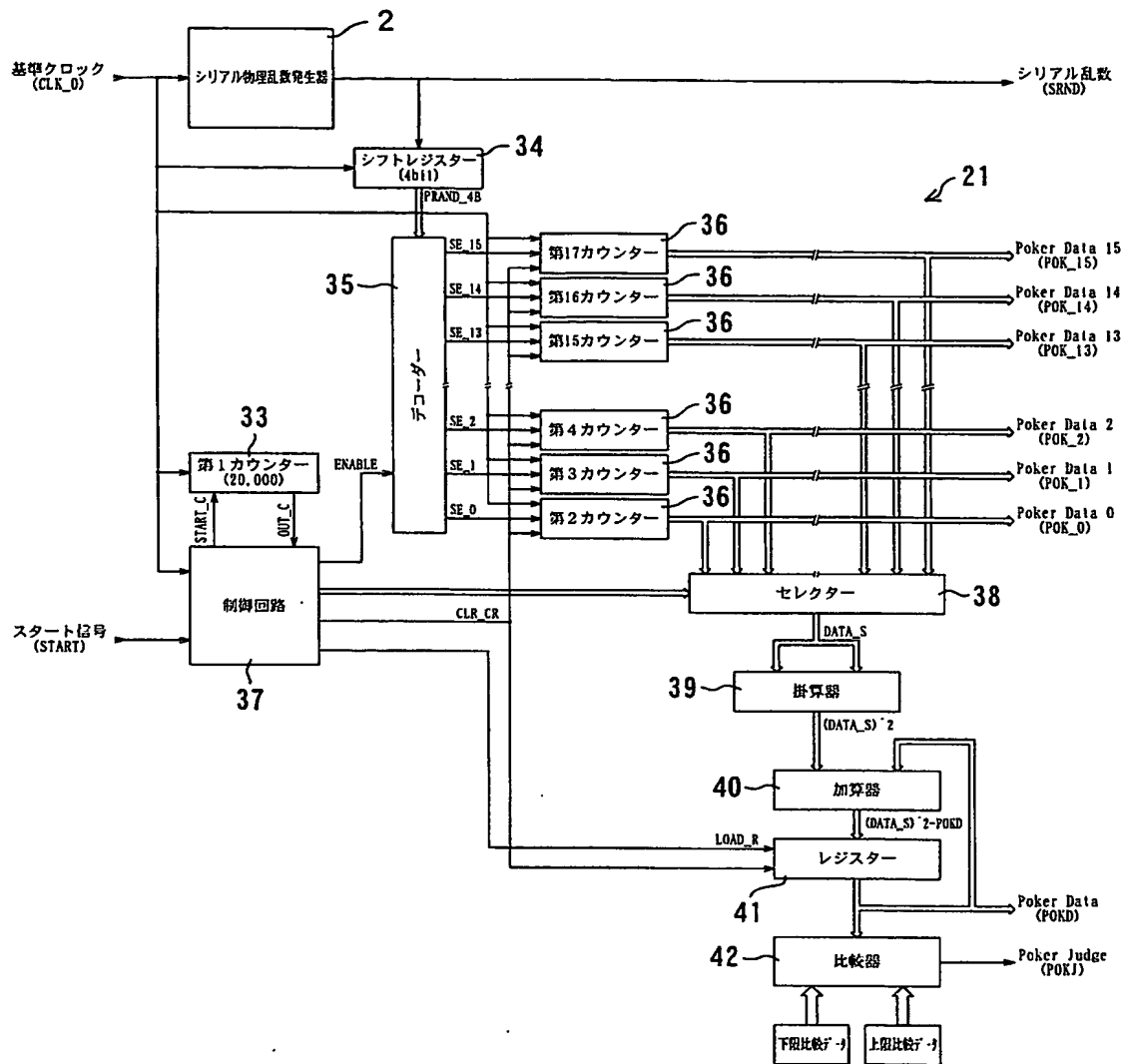
【図 4】



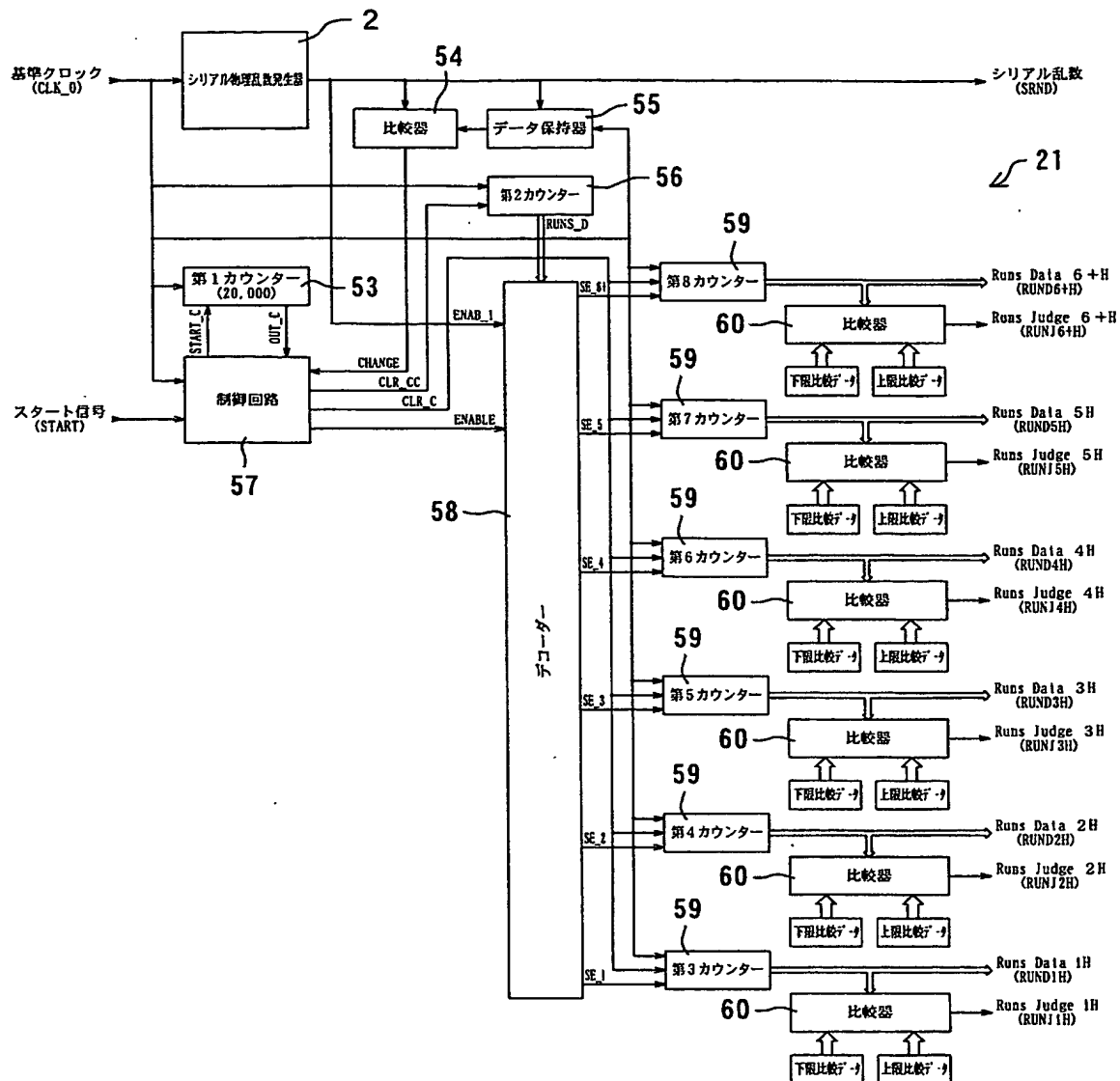
【図 5】



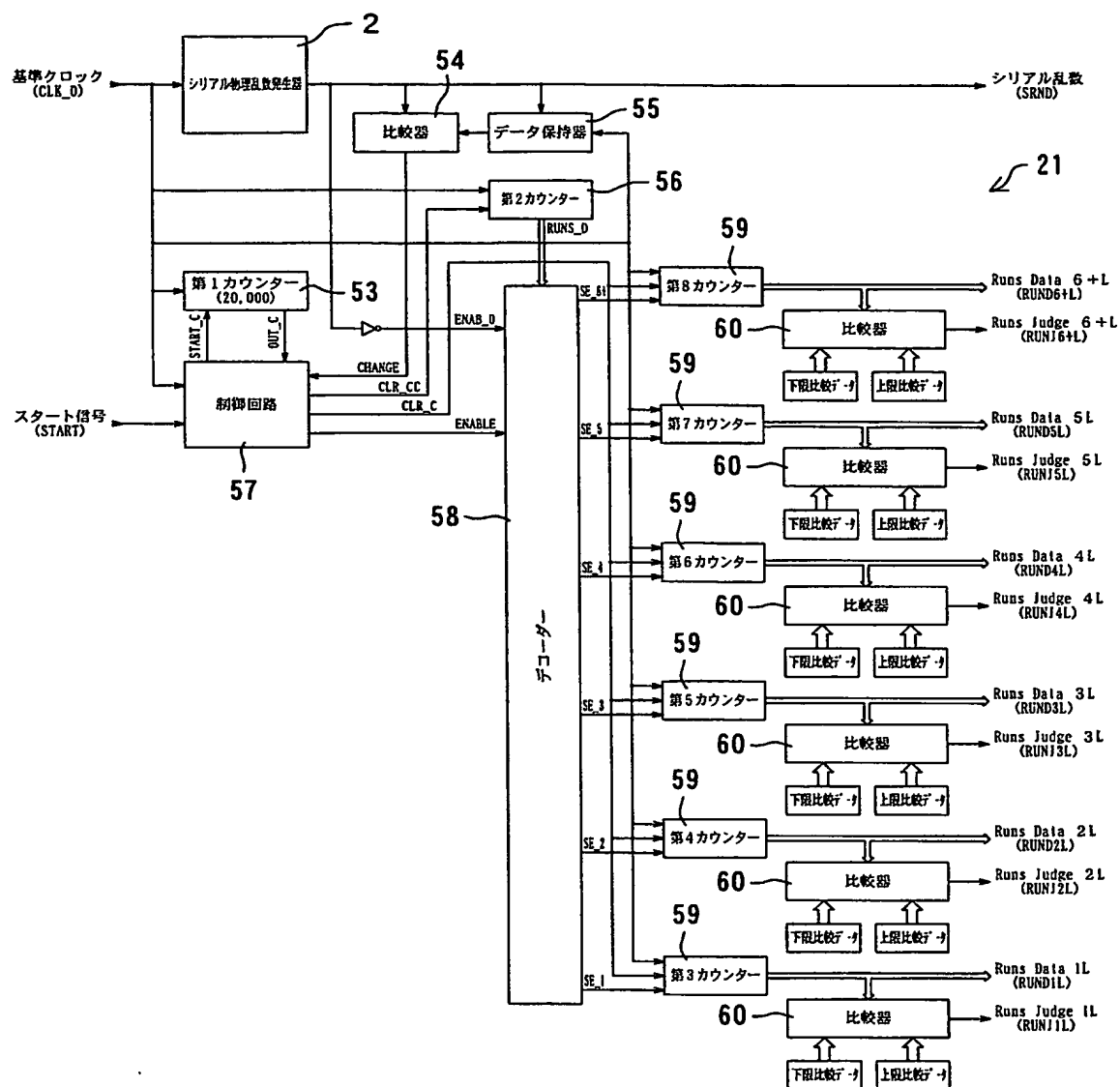
【図 6】



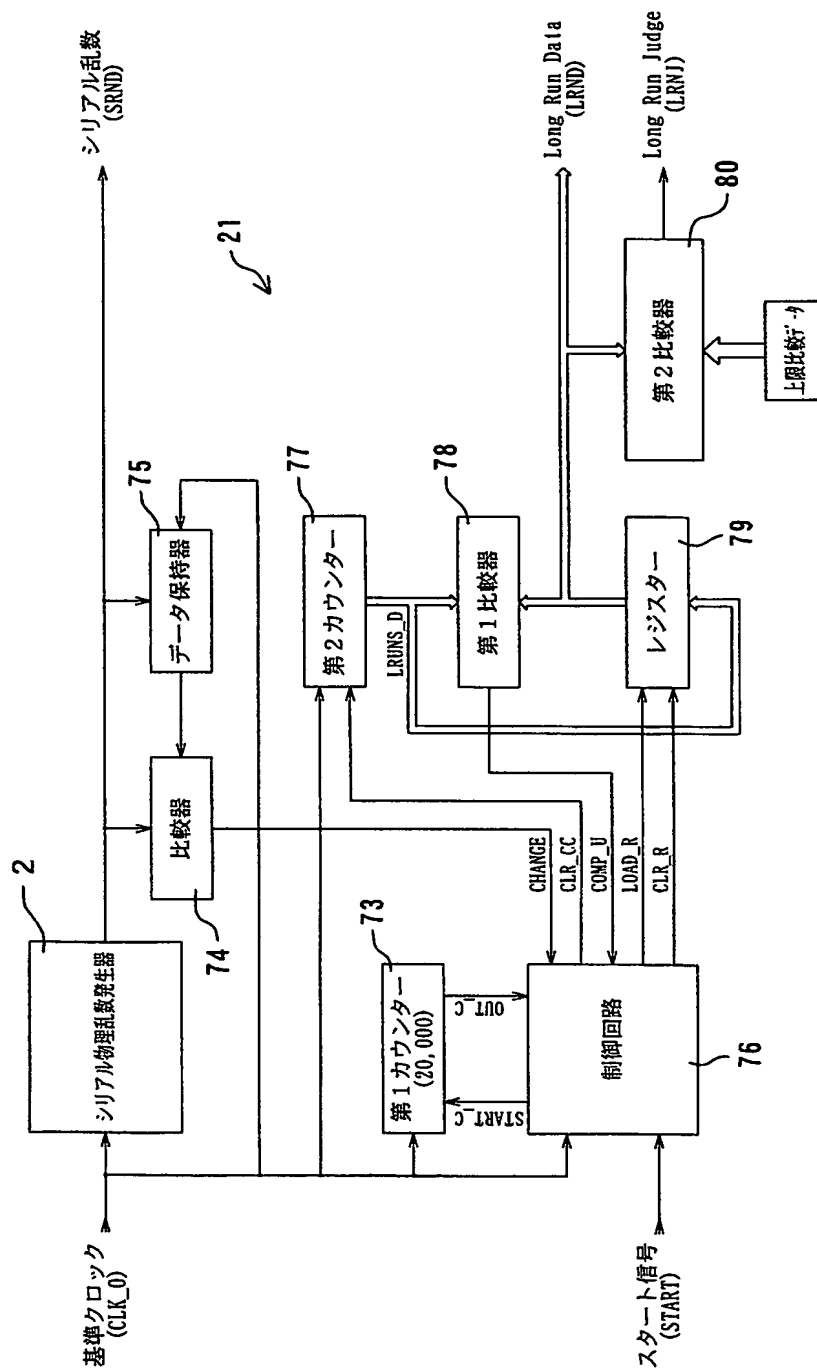
【図 7】



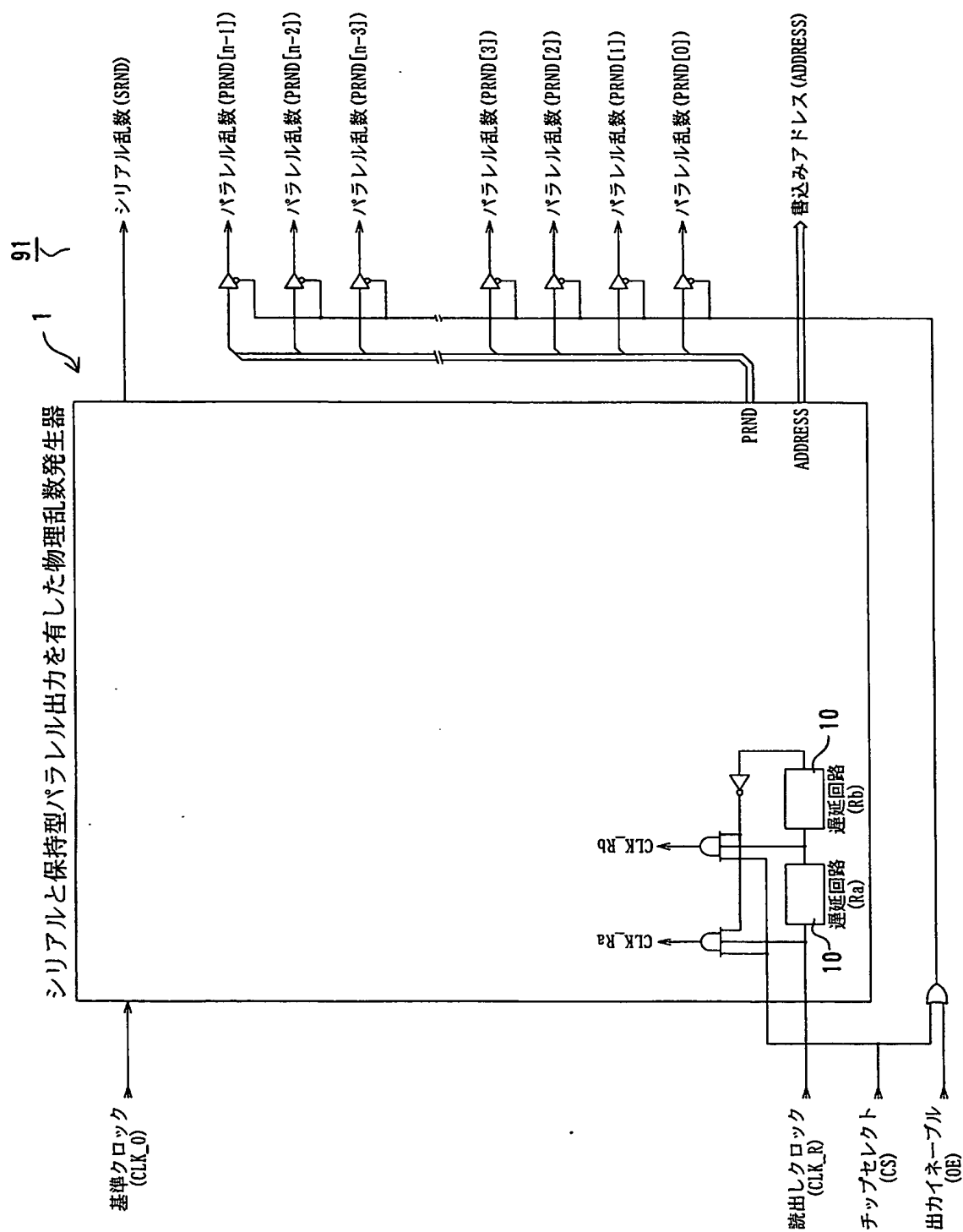
【図 8】



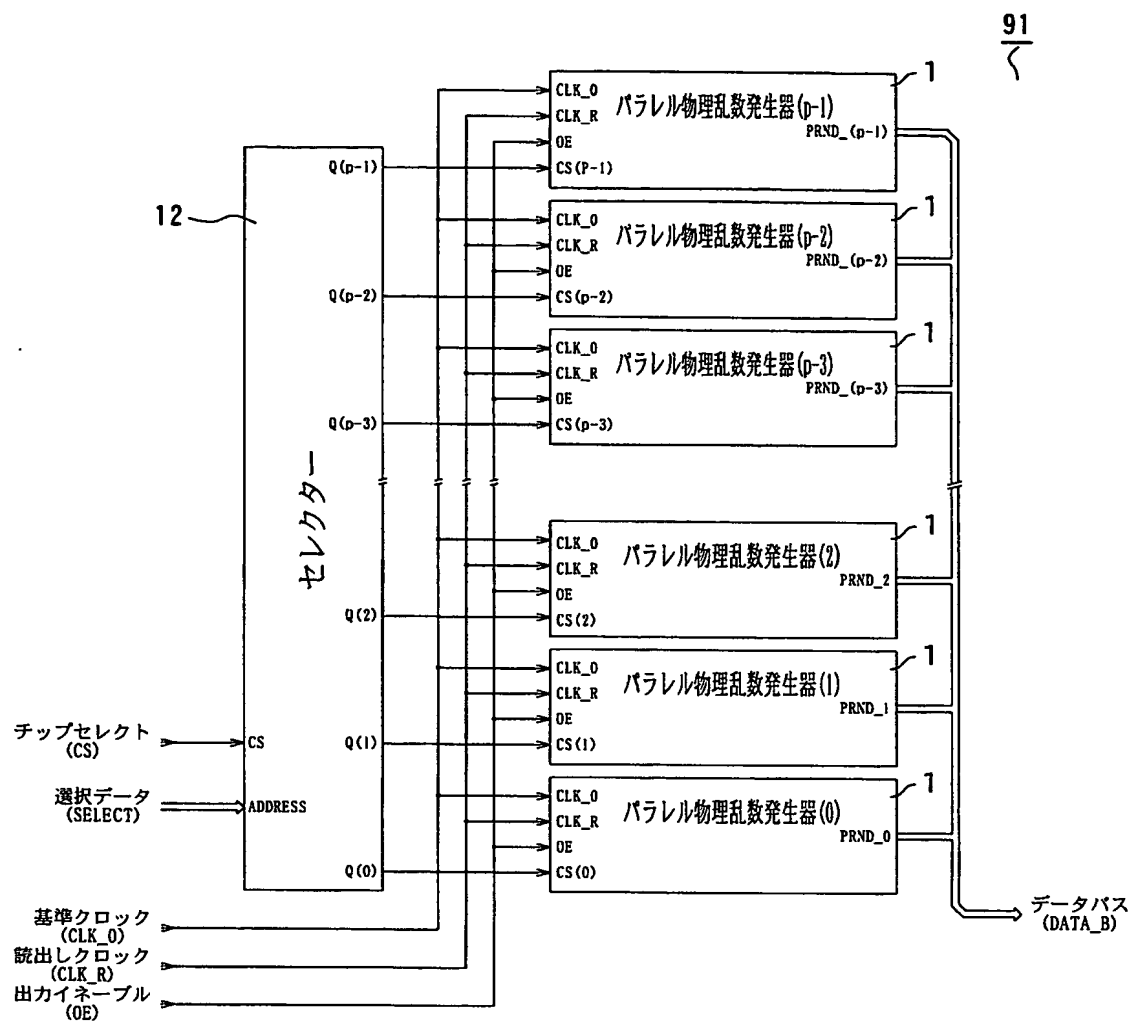
【図9】



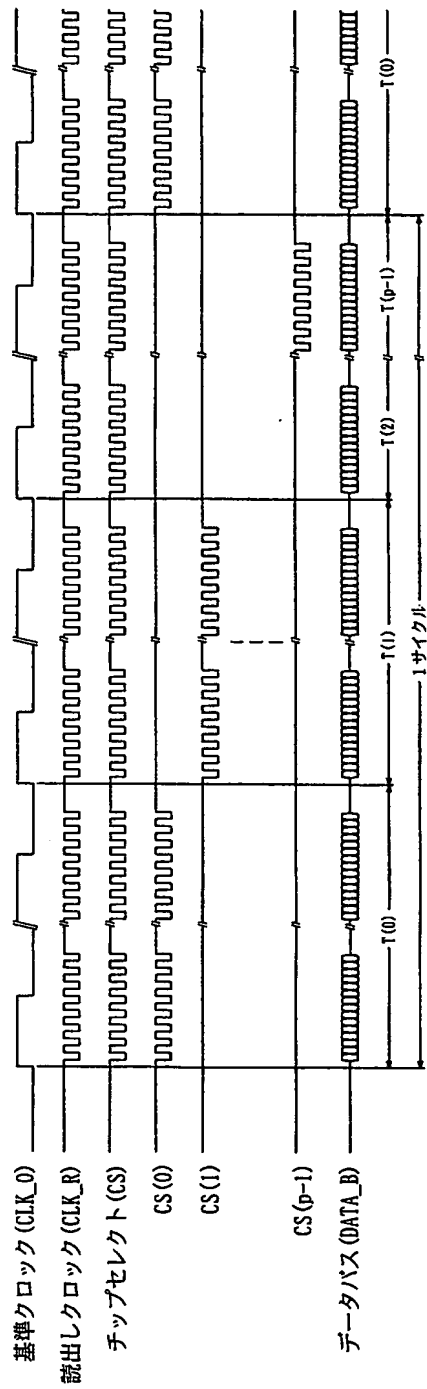
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 セキュリティーなどの用途に用いる物理乱数発生装置において、単体での乱数利用効率を高め、複数の物理乱数 IC を組み上げて乱数を高速に発生させ、乱数の質を容易に確認できるようにする。

【解決手段】 物理乱数発生器 1 を有する物理乱数発生装置であって、物理乱数発生器 1 が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器 2 を備える。シリアル乱数をパラレル乱数に変換するシフトレジスタ 4 を備え、パラレル乱数を保持しうる複数個のレジスタ 5 を備える。パラレル乱数が生成される度にレジスタ 5 に順次パラレル乱数を保持し、かつ、読出しクロック信号に応じてレジスタ 5 からパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスタ 5 に他のレジスタ 5 からパラレル乱数をシフトさせて内容を逐次更新する制御回路 6 を備える。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願 2003-101085
受付番号	50300562148
書類名	特許願
担当官	第八担当上席 0097
作成日	平成15年 4月 7日

<認定情報・付加情報>

【提出日】	平成15年 4月 4日
-------	-------------

次頁無

特願 2003-101085

出 願 人 履 歴 情 報

識別番号

[000237721]

1. 変更年月日

2001年 1月16日

[変更理由]

名称変更

住 所

東京都港区新橋5丁目36番11号

氏 名

エフ・ディー・ケイ株式会社

2. 変更年月日

2003年 8月13日

[変更理由]

名称変更

住 所

東京都港区新橋5丁目36番11号

氏 名

F D K 株式会社